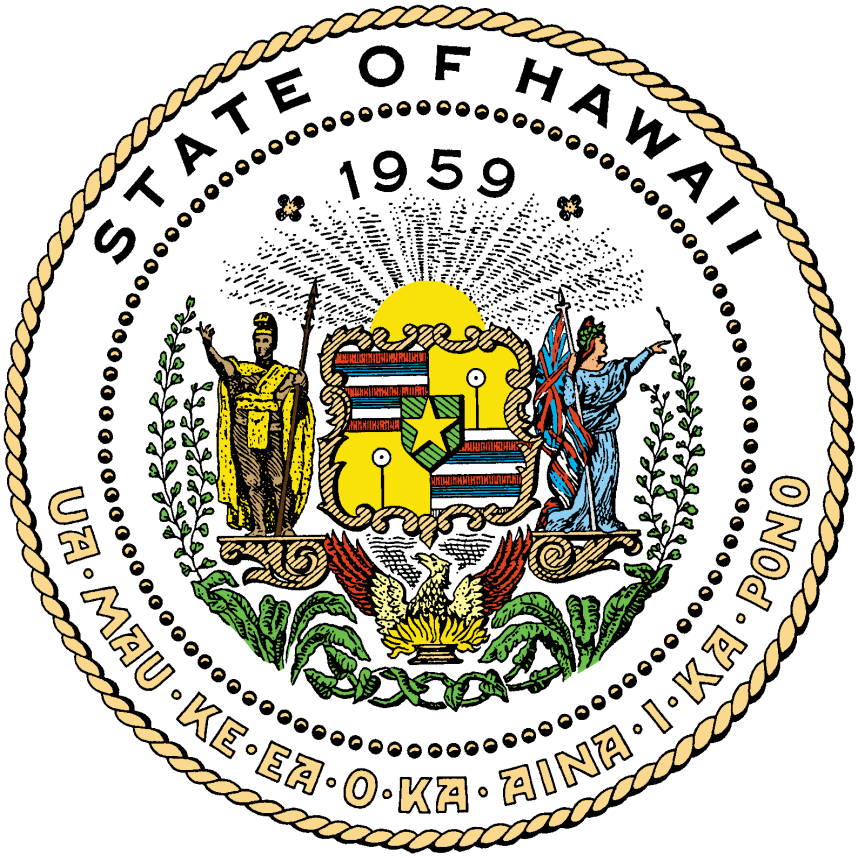
Number 08.00



COMPUTER AND NETWORK RESOURCES ACCEPTABLE USE POLICY

August 2001

TABLE OF CONTENTS

Department of Accounting and General Services
Information and Communication Services Division
Information Technology Standards

1 INTRODUCTION

This document was developed by the Department of Accounting and General Services (DAGS), Information and Communication Services Division (ICSD) for the State of Hawaii Executive Branch to establish standards for acceptable use of the computer and network resources in an information processing environment.

This Policy is in accord with and supported by the statewide IT Standards relating to computer and data security that were approved and published by DAGS, ICSD. These standards are identified as 08.01 IT Security Overview; 08.02 Information Security; and 08.04 Network Security. The IT Standards are available through DAGS/ICSD, Project Planning and Management Office.

1.1 Scope

Computer and network resources include all hardware, software, documentation, programs, information, data, and other devices that are owned by or are under the operational jurisdiction of the DAGS. These resources include those that enable remote and local communication or access between various platforms and environments such as the mainframe, minicomputers, servers, LANS, and personal computers. Computer and network resources are hereinafter referred to as information resources.

1.2 Applicability

This Policy applies to individuals who use or access the DAGS, ICSD computer and network resources. These individuals are referred to as “Users”. Users include employees of DAGS; non-employees such as volunteers, contractors, vendors; personnel from other State agencies; personnel from other governmental jurisdictions; and members of the general public.

1.3 Purpose

The purpose of this Policy is to ensure proper use of DAGS, ICSD computer and network resources. This Policy augments the State’s “Policy and Guidelines on the Use of the State of Hawaii Electronic Mail System”, a memo dated February 2, 1998.

1.4 Comments and Suggestions

The Department may amend or revise this Policy from time to time as the need

arises, with or without prior notice. The DAGS Personnel Office will provide the various departmental agencies with copies of the amended or revised Policy for circulation among users, for posting on official bulletin boards, and for posting on the DAGS web site.

Comments, suggestions, and recommendations are welcomed. Please send them to:

Information and Communication Services Division
Planning and Project Management Office
1151 Punchbowl Street, Room B10
Honolulu, Hawaii 96813

Telephone: 586-1920

2 GENERAL INFORMATION

2.1 Benefits

The use of computer and network resources, such as electronic communications for email and voice mail, Internet access, and electronic transfer of information provide the Department with a greatly enhanced ability to improve productivity, increase efficiency, and deliver a high quality of work.

2.2 Permission and Acceptance

The Comptroller is the authorizing authority for use of information resources. The Comptroller may delegate the responsibility and duties relating to the use of information resources to the Deputy Comptroller, Division Heads, and Staff Officers. However, the ultimate responsibility for use of the Department's information resources rests with the Comptroller.

The use of information resources constitutes consent by a User to all the terms and conditions of this Policy.

2.3 No Expectancy of Privacy

A User should be aware that there is no proprietary interest and no reasonable expectation of privacy while using any of the information resources provided by the Department, including but not limited to word processing documents, electronic and voice mail, and Internet access. The Department views all information processed by and stored on the Department's information resources

as owned by or under the custodial authority of the Department and may obtain access to the information at any time.

3 USER RESPONSIBILITIES

A User is expected to become familiar with this and other supporting and applicable policies. Questions relating to the applicability of this policy may be directed to the Department's Personnel Office. Questions relating to the technical aspects of the computer usage may be directed to the ICSD, Project Planning and Management Office.

3.1 User Duties

3.1.1 Waste of Information Resources

A User must not perform acts that waste information resources unfairly or to monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amount of time on the Internet, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic. Since audio, video, and picture files require significant storage space and transfer time, files of this or similar type may not be downloaded unless they are work-related.

A User should not tie up resources and create security risks by remaining logged on while away from his or her computer. Standards relating to terminal activity and when a User should log off can be found in 08.02 Information Security, Section 5 Computer Logon Access.

A User should routinely delete outdated or otherwise unnecessary electronic communication and computer files. These deletions free up information resources and help to keep systems running more efficiently and smoothly.

3.1.2 Lawful Actions and Reporting Misuse of Information Resources

A User is expected to act lawfully, ethically, respectfully, and responsibly in the use of the Department's information resources. A User who encounters or receives unlawful, unethical, or questionable material should immediately report the incident. The incident should be reported to the supervisor or manager, who should notify the Division Head, who in turn should report the incident to the ICSD Division Head.

3.1.3 Protection of Information Resources

A User is expected to take all reasonable precautions to protect the Department's information resources from unauthorized access, use, disclosure, modification, duplication, and/or destruction. Therefore, a User must employ the access controls, and other security measures that the Department has provided and must take prudent and reasonable steps to limit unauthorized access to information resources. A User is expected to assist and cooperate in the protection of the information resources.

3.1.4 Safeguarding Access Via the Internet

Accessing the Internet directly from network enabled equipment by modem is strictly prohibited. Attaching modems to equipment that is not connected to the Department's network requires prior approval from the Division Head.

3.1.5 Safeguarding Passwords

Passwords are used to protect information resources. Therefore, a User should not employ passwords that are easy to guess. This includes but is not limited to the use of common words or names. For further information regarding the use of logon-ids and passwords, see: IT Standard 08.02 Information Security, Section 5.1 Logon-ID/Password Policy.

3.1.6 Prevention of Viruses and Disruptive Code

A User must scan all files obtained from external sources for viruses or signs of other malicious code before accessing the information. This includes but is not limited to diskettes brought from home, or provided by clients or vendors; files downloaded from Internet newsgroups, bulletin boards, or other services; and files received as email attachments.

3.1.7 Protecting Logon Access and Passwords

A User must keep passwords confidential. A User should not divulge a password to anyone, or write it down, or place it where it can be seen or found. Each User is responsible for any and all actions and consequences of authorized use of his or her username, logonid, and password by individuals such as family members and co-workers.

If a User who suspects or discovers that someone is using a logonid without permission, it should be immediately reported to the User's supervisor, or the Division Head. The logonid that is being misused should not be used until further instruction is received from departmental management saying that the logonid can be used.

3.1.8 Maintaining Security Classifications

An electronic communication, such as email, whose content or attached files carry a security classification should be clearly marked with that classification, i.e. "confidential", "proprietary information", "attorney client privilege", or whatever other classification is assigned. Any electronic communication that has been assigned a security classification is to be handled, retained and disposed of according to applicable regulations.

Classified information should only be transmitted or disclosed through electronic communication media to another party who is entitled to receive and view that information.

3.1.9 Safguarding Information on Personal Computers

A User is responsible for protecting information resources to which the User has access. This includes but is not limited to making backup copies of files and data on PC hard drives; protecting access to Departmental and other data that is stored on a PC; utilizing a locked drawer to secure diskettes that contain classified, sensitive and/or critical data; maintaining the security of hard copy printouts of classified information.

3.2 Personal Usage

An employee of the Department is allowed to have incidental personal usage of information resources if such privilege does not adversely affect the program's operations, or does not cause harm or embarrassment to the Department. Any personal use of information resources by an employee should be on the employee's own time and should not interfere with job duties. Good judgement must be exercised in using the Department's information resources, and should

be limited. An employee is not authorized to make personal, non-business use of information resources that result in additional charge to the Department, and is not allowed to engage in the prohibited activities as described in Section VII. It is the employee's responsibility to be aware of and responsible for any additional cost that is involved. Since electronic communication media such as Internet and electronic mail identifies a User, an employee engaging in personal use of the Department's information resources should make it clear that such activity or communication is not being used for official business of the Department.

3.3 Prohibited Activities

3.3.1 Unauthorized Access to Files and Directories

A User has access rights to files and directories associated with the user's logonid and dependant upon the user's work-related or business requirements. A User is prohibited from circumventing the security controls of the Department's information resources. Accessing directories and files of other Users in order to read, browse, modify, copy, or delete any data or information without the explicit approval of the individual User or from the appropriate departmental management is strictly prohibited.

Examples of such activities include but are not limited to cracking other User's passwords, decoding encrypted files, and using programs to secretly penetrate computer and information systems.

3.3.2 Unauthorized Use of Copyrighted or Proprietary Materials

A User is prohibited from illegally copying material that is protected under copyright law or from making such material available to others for copying. The Department is the sole owner, custodian, or licensed user of software that is installed on its information resources. According to U.S. Copyright Law, illegal reproduction of software is subject to civil monetary damages and criminal penalties, including fines and imprisonment.

A User is prohibited from sending (uploading) or receiving (downloading) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior approval from the Comptroller or the individual delegated by the Comptroller to make such approval.

A User who does not know if information is copyrighted, proprietary, or otherwise inappropriate for transfer, should consult with the User's supervisor to get approval before transferring the information.

3.3.3 Use of Computer Resources for Games

A User is prohibited from using the Department's information resources for Internet connection to download games or other entertainment software, and from using the Internet connection to play games.

3.3.4 Use of Software Not Provided by DAGS

A User is prohibited from installing software, such as commercial, shareware, and freeware, on any computer without the explicit approval of the Division Head or Staff Officer. Such approval will be based upon whether or not the software has a clear business purpose, has been approved by use by the appropriate IT personnel, is consistent with the technology infrastructure, and has been scanned for virus and other malicious code.

3.3.5 Use for Profit and Solicitation

A User is prohibited from using the Department's information resources for any personal or private financial gain; commercial or profit-making activities; and political, religious or other solicitations.

3.3.6 Unlawful and Unethical Conduct

A User is expected to conduct himself or herself in a professional manner and to exercise courtesy when using any electronic communication media. A User should exercise the same degree of care, judgement, and responsibility in composing and transmitting electronic communications as would be done when composing communication that is to be printed. A User should assume that an electronic message would be saved, and reviewed by someone other than the intended recipients.

A User is prohibited from using the Department's information resources to access, download from the Internet, display, or store any information that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, libelous, defamatory, or otherwise unlawful, inappropriate, offensive. This includes material concerning sex, race, color, national origin, age, disability, or other characteristics protected by law.

The Department's Sexual Harassment Policy, and the Equal Employment Opportunity and Affirmative Action Policy apply fully to the use of

information resources. A User is prohibited from any actions the employ the Department's information resources to violate these policies.

A User is prohibited from using information resources for any other unlawful or unethical purposes, including but not limited to pornography, violence, or gambling.

A User is prohibited from using profanity or vulgarity when using any information resources.

A User is prohibited from making defamatory comments or taking actions, such as forwarding of electronic mail, which facilitate the "publication" of such comments.

3.3.7 Attacking the System

A User must not attempt to degrade the performance of the Department's information resources or to subvert them in any other way. Activities which are expressly prohibited include but are not limited to the following: deliberately crashing any computer system; using software that is designed to destroy data, facilitate unauthorized access to information resources, or disrupt computing processes in any way; and using invasive software that may cause viruses.

3.3.8 Theft

A User is prohibited from removing any hardware, software, attached peripherals, supplies, and documentation without the expressed approval from the respective Division Head or Staff Officer. Further, a user is prohibited from using diskettes, manuals, or other means to obtain restricted information.

3.3.9 Misrepresentation

A User is prohibited from making unauthorized statements or commitments on behalf of the Department, or posting an unauthorized home page or similar web site.

4 DISCLAIMER OF LIABILITY FOR INTERNET USE

A User who accesses the Internet does so at his or her own risk. The Department is not responsible for material viewed or downloaded by a User from the Internet. Even

innocuous search requests may lead to sites with highly offensive content. In general, it is difficult to avoid at least some contact with this material while using the Internet. A User is cautioned that pages might include offensive, sexually explicit, and inappropriate material. In addition, having an electronic mail address on the Internet may lead to receipt of unsolicited electronic mail that has offensive content.

5 MONITORING AND ENFORCEMENT

The Department is the Owner or Custodian of data and information stored on, processed by, or transiting through the Department's computer and network resources. The Department must safeguard the information resources under its care. To do so, the Department needs to ensure compliance with applicable rules, regulations, and policies; monitor the performance of the information resources; keep the computing environment free from intrusion and destructive code; conduct investigations; and perform other such information security tasks.

The Department may at any time, and without prior notice, examine data and information. The Department has the right to monitor any and all of the aspects of the computing and networking resources. This includes, but is not limited to, monitoring access by a User to the Internet sites that are visited; viewing the contents of electronic mail, chat groups, or news groups; and inspecting materials downloaded or uploaded by a User.

The Department reserves the right to revoke access to information resources, to override a User's password without notice, or to require a user to disclose passwords and/or codes to facilitate access to information resources.

Violation of this or any other policy by a User may result in immediate revocation of access privileges. There may also be disciplinary action that may include termination, and/or civil and criminal liability. See IT Security Standard 08.01, IT Security Overview, Section 4 Security Enforcement.